

REMARKS ON LOW WEIGHT CODEWORDS OF GENERALIZED AFFINE AND PROJECTIVE REED-MULLER CODES

S. BALLEST AND R. ROLLAND

ABSTRACT. A brief survey on low weight codewords of generalized Reed-Muller codes and projective generalized Reed-Muller codes is presented. In the affine case some information about the words that reach the second distance is given. Moreover the second weight of the projective Reed-Muller codes is estimated, namely a lower bound and an upper bound of this weight are given.

1. INTRODUCTION - NOTATIONS

This paper proposes an overview of the low weight codewords of generalized Reed-Muller codes and projective generalized Reed-Muller codes called respectively GRM codes and PGRM codes. It includes a focus on their minimum distances as well as the characterization of the codewords reaching these weights. It also includes a study of the second weight, namely the weight which is just above the minimal distance. The second weight is also called the next-to-minimum weight.

The second weight is now known for GRM codes (see [4]), but is not known for PGRM codes. Many results concerning this area are here and there in various papers. In this situation, a comprehensive overview is needed. This is what we do at first. Then we study some results concerning the codewords of a GRM code reaching the second weight. These codewords are known when $1 \leq d \leq \frac{q}{2}$ (cf. [8], [18]). For other values of d we prove that an irreducible, non-absolutely irreducible polynomial cannot reach the second weight. For $d < q - 1$ we improve the previous result. More precisely we show that a polynomial having a factor of degree $d \geq 2$ which is irreducible, non-absolutely irreducible, cannot reach the second weight.

We then determine an upper bound and a lower bound for the second weight of a PGRM code which is not already known.

1.1. Polynomials and homogeneous polynomials. Let \mathbb{F}_q be the finite field with q elements and $n \geq 1$ an integer. We denote respectively by $\mathbb{A}^n(q)$ and $\mathbb{P}^n(q)$ the affine space and the projective space of dimension n over \mathbb{F}_q .

Let $\mathbb{F}_q[X_1, X_2, \dots, X_n]$ be the algebra of polynomials in n variables over \mathbb{F}_q . If f is in $\mathbb{F}_q[X_1, X_2, \dots, X_n]$ we denote by $\deg(f)$ its total degree and by $\deg_{X_i}(f)$ its partial degree with respect to the variable X_i .

Denote by $\mathcal{F}(q, n)$ the space of functions from \mathbb{F}_q^n into \mathbb{F}_q . It is known that any function in $\mathcal{F}(q, n)$ is a polynomial function. More precisely there is a surjective

Date: February 28, 2013.

2000 Mathematics Subject Classification. 11G25, 11T71.

Key words and phrases. code, codeword, finite field, generalized Reed-Muller code, homogeneous polynomial, hyperplane, hypersurface, minimal distance, next-to-minimal weight, polynomial, projective Reed-Muller code, second distance, weight.

linear map T from $\mathbb{F}_q[X_1, X_2, \dots, X_n]$ onto $\mathcal{F}(q, n)$ mapping any polynomial on its associated polynomial function:

$$\begin{array}{ccc} T : \mathbb{F}_q[X_1, X_2, \dots, X_n] & \rightarrow & \mathcal{F}(q, n) \\ f & \mapsto & T(f) \end{array}$$

where $T(f)(X) = f(X)$ is the evaluation of the polynomial f at the point $X = (X_1, X_2, \dots, X_n)$. The map T is not injective and has for kernel the ideal generated by the n polynomials $X_i^q - X_i$:

$$\text{Ker}(T) = (X_1^q - X_1, X_2^q - X_2, \dots, X_n^q - X_n).$$

Any element of the quotient $\mathbb{F}_q[X_1, X_2, \dots, X_n]/\text{Ker}(T)$ can be represented by a unique reduced polynomial f , namely such that for any variable X_i the following holds:

$$\deg_{X_i}(f) \leq q - 1.$$

We denote by $\mathcal{RP}(q, n)$ the set of reduced polynomials in n variables over \mathbb{F}_q . Then, the map T restricted to $\mathcal{RP}(q, n)$ is one to one, namely each function of $\mathcal{F}(q, n)$ can be uniquely represented by a reduced polynomial in $\mathcal{RP}(q, n)$.

Let d be a positive integer. We denote by $\mathcal{RP}(q, n, d)$ the set of reduced polynomials P such that $\deg(P) \leq d$. Remark that if $d \geq n(q - 1)$ the set $\mathcal{RP}(q, n, d)$ is the whole set $\mathcal{RP}(q, n)$.

Let $\mathcal{H}(q, n + 1, d)$ the space of homogeneous polynomials in $n + 1$ variables over \mathbb{F}_q with total degree d . The decomposition

$$\mathbb{F}_q[X_0, X_1, X_2, \dots, X_n] = \bigoplus_{d \geq 0} \mathcal{H}(q, n + 1, d)$$

provides $\mathbb{F}_q[X_0, X_1, X_2, \dots, X_n]$ with a graded algebra structure. Let \mathcal{J}_d be the subspace of polynomials f in $\mathcal{H}(q, n + 1, d)$ such that $f(X) = 0$ for any $X \in \mathbb{F}_q^{n+1}$ and denote by \mathcal{J} the homogeneous ideal

$$\mathcal{J} = \bigoplus_{d \geq 0} \mathcal{J}_d.$$

It is known (cf. [14] or [15]) that the ideal \mathcal{J} is the homogeneous ideal generated by the polynomials $X_i^q X_j - X_i X_j^q$ where $0 \leq i < j \leq n$.

1.2. Generalized Reed-Muller codes. Let d be an integer such that $1 \leq d < n(q - 1)$. The generalized Reed-Muller code (GRM code) of order d over \mathbb{F}_q is the following subspace of $\mathbb{F}_q^{(q^n)}$:

$$\begin{aligned} \text{RM}_q(d, n) = \\ \left\{ (f(X))_{X \in \mathbb{F}_q^n} \mid f \in \mathbb{F}_q[X_1, \dots, X_n] \text{ and } \deg(f) \leq d \right\}. \end{aligned}$$

It may be remarked that the polynomials f determining this code are viewed as polynomial functions. Hence each codeword is associated with a unique reduced polynomial in $\mathcal{RP}(q, n, d)$.

Let us denote by $Z_a(f)$ the set of zeros of f (where the index a stands for “affine”). From a geometrical point of view $Z_a(f)$ is an affine algebraic hypersurface in \mathbb{F}_q^n and the number of points $N_a(f) = \#Z_a(f)$ of this hypersurface (the number of zeros of f) is connected to the weight $W_a(f)$ of the associated codeword by the following formula:

$$W_a(f) = q^n - N_a(f).$$

The code $\text{RM}_q(d, n)$ has the following parameters (cf. [10], [1, p. 72]) (where the index a stands for “affine code”):

- (1) length $m_a(q, n, d) = q^n$,
- (2) dimension

$$k_a(q, n, d) = \sum_{t=0}^d \sum_{j=0}^n (-1)^j \binom{n}{j} \binom{t - jq + n - 1}{t - jq},$$

- (3) minimum distance $W_a^{(1)}(q, n, d) = (q - b)q^{n-a-1}$, where a and b are the quotient and the remainder in the Euclidean division of d by $q - 1$, namely $d = a(q - 1) + b$ and $0 \leq b < q - 1$.

We denote by $N_a^{(1)}(q, n, d)$ the maximum number of zeros for a non-null polynomial function of degree $\leq d$ where $1 \leq d < n(q - 1)$, namely

$$N_a^{(1)}(q, n, d) = q^n - W_a^{(1)}(q, n, d) = q^n - (q - b)q^{n-a-1}.$$

Remark 1.1. Be careful not to confuse symbols. With our notations, the Reed-Muller code of order d has length $m_a(q, n, d)$, dimension $k_a(q, n, d)$ and minimum distance $W_a^{(1)}(q, n, d)$. Namely it is an

$$\left[m_a(q, n, d), k_a(q, n, d), W_a^{(1)}(q, n, d) \right] - \text{code}.$$

The integer n is the number of variables of the polynomials defining the words and the order d is the maximum total degree of these polynomials.

The minimum distance of $\text{RM}_q(d, n)$ was given by T. Kasami, S. Lin, W. Peterson in [10]. The words reaching this bound were characterized by P. Delsarte, J. Goethals and F. MacWilliams in [6] and are described in the following theorem:

Theorem 1.2 (Delsarte, Goethals, MacWilliams). *The maximum number of \mathbb{F}_q -rational points, for an algebraic hypersurface V of degree d in the affine space of dimension n which is not the whole space \mathbb{F}_q^n is attained if and only if:*

$$V = \left(\bigcup_{i=1}^a \left(\bigcup_{j=1}^{q-1} V_{i,j} \right) \right) \left(\bigcup_{j=1}^b W_j \right) \text{ where } d = a(q - 1) + b,$$

with $0 \leq b < q - 1$ and where the $V_{i,j}$ and W_j are d distinct hyperplanes defined on \mathbb{F}_q such that for each fixed i the $V_{i,j}$ are $q - 1$ parallel hyperplanes, the W_j are b parallel hyperplanes and the $a + 1$ distinct linear forms directing these hyperplanes are linearly independent.

1.3. Projective generalized Reed-Muller codes. The case of projective codes is a bit different, because homogeneous polynomials do not define in a natural way functions on the projective space. Let d be an integer such that $1 \leq d \leq n(q - 1)$. The projective generalized Reed-Muller code of order d (PGRM code) was introduced by G. Lachaud in [12]. Let S a subset of \mathbb{F}_q^{n+1} constituted by one point on each punctured vector line of \mathbb{F}_q^{n+1} . Remark that any point of the projective space $\mathbb{P}^n(q)$ has a unique coordinate representation by an element of S .

The projective Reed-Muller code $\text{PRM}_q(n, d)$ of order d over $\mathbb{P}^n(q)$ is constituted by the words $(f(X))_{X \in S}$ where $f \in \mathcal{H}(q, n+1, d)$ and the null word:

$$\text{PRM}_q(n, d) = \left\{ (f(X))_{X \in S} \mid f \in \mathcal{H}(q, n+1, d) \right\} \cup \{(0, \dots, 0)\}.$$

This code is dependent on the set S chosen to represent the points of $\mathbb{P}^n(q)$. But the main parameters are independent of this choice. Following [12] we can choose

$$S = \cup_{i=0}^n S_i,$$

where $S_i = \{(0, \dots, 0, 1, X_{i+1}, \dots, X_n) \mid X_k \in \mathbb{F}_q\}$. Subsequently, we shall adopt this value of S to define the code $\text{PRM}_q(n, d)$.

For a homogeneous polynomial f let us denote by $Z_h(f)$ the set of zeros of f in the projective space $\mathbb{P}^n(q)$ (where the index h stands for “projective”). From a geometrical point of view, an element $f \in \mathcal{H}(q, n+1, d)$ defines a projective hypersurface $Z_h(f)$ in the projective space $\mathbb{P}^n(q)$. The number $N_h(f) = \#Z_h(f)$ of points of this projective hypersurface is connected to the weight $W_h(f)$ of the corresponding codeword by the following relation:

$$W_h(f) = \frac{q^{n+1} - 1}{q - 1} - N_h(f).$$

The parameters of $\text{PRM}_q(n, d)$ are the following (cf. [21]) (where the index h stands for “projective code”):

- (1) length $m_h(q, n, d) = \frac{q^{n+1} - 1}{q - 1}$,
- (2) dimension

$$k_h(q, n, d) = \sum_{\substack{t = d \bmod q-1 \\ 0 < t \leq r}} \left(\sum_{j=0}^{n+1} (-1)^j \binom{n+1}{j} \times \binom{t - jq + n}{t - jq} \right),$$

- (3) minimum distance: $W_h^{(1)}(q, n, d) = (q - b)q^{n-a-1}$ where a and b are the quotient and the remainder in the Euclidean division of $d - 1$ by $q - 1$, namely $d - 1 = a(q - 1) + b$ and $0 \leq b < q - 1$.

We denote by $N_h^{(1)}(q, n, d)$ the maximum number of zeros for a non-null homogeneous polynomial function of degree d where $1 \leq d \leq n(q - 1)$, namely

$$N_h^{(1)}(q, n, d) = \frac{q^{n+1} - 1}{q - 1} - W_h^{(1)}(q, n, d) = \frac{q^{n+1} - 1}{q - 1} - (q - b)q^{n-a-1}.$$

2. MINIMAL DISTANCE AND CORRESPONDING CODEWORDS

2.1. The affine case: GRM codes. For the affine case recall that we write the degree d in the following form:

$$(1) \quad d = a(q-1) + b \quad \text{with } 0 \leq b < q-1.$$

The minimum distance of a GRM code was given by T. Kasami, S. Lin, W. Peterson in [10]. The words reaching this bound (i.e. the polynomials reaching the maximal number of zeros) were characterized by P. Delsarte, J. Goethals and F. MacWilliams in [6]. As indicated in [6] the polynomials reaching this bound can be written:

$$(2) \quad P(X) = w_0 \prod_{i=1}^a (1 - (l_i(X) - w_i)^{q-1}) \prod_{j=1}^b (l_{a+1}(X) - w'_j)$$

where $X \in \mathbb{F}_q^n$, the w'_j in the last b factors are distinct elements of \mathbb{F}_q , the w_i are arbitrary elements of \mathbb{F}_q with $w_0 \neq 0$ and l_i are $a+1$ linearly independent linear forms on \mathbb{F}_q^n .

Give here the geometric interpretation of such a polynomial f reaching the maximal number of zeros. The hypersurface defined by f is the following arrangement of hyperplanes:

- (1) a blocks of $q-1$ parallel hyperplanes, each of them directed by one of the a first linearly independent linear forms l_i ,
- (2) one block of b parallel hyperplanes directed by l_{a+1} .

Such a hypersurface will be called a maximal hypersurface and the associated polynomial is called a maximal polynomial. The corresponding weight is the minimal weight.

2.2. The projective case: PGRM codes. Let us denote respectively by $W_h^{(1)}(q, n, d)$ and $W_h^{(2)}(q, n, d)$ the first and second weight of the projective Reed-Muller code.

Lemma 2.1. *Let $d > n(q-1)$. Then for any N such that $0 \leq N \leq \frac{q^{n+1}-1}{q-1}$ there exists a homogeneous polynomial of degree d in $n+1$ variables having N zeros in $\mathbb{P}^n(q)$. In particular $W_h^{(1)}(q, n, d) = 1$ and $W_h^{(2)}(q, n, d) = 2$.*

Proof. let

$$\omega = (0 : 0 : \dots : 1 : \omega_{j+1} : \dots : \omega_n)$$

be a point in $\mathbb{P}^n(q)$ and

$$\begin{aligned} f_\omega^d(X) = & X_j^{d-n(q-1)} \prod_{i=0}^{j-1} (X_j^{q-1} - X_i^{q-1}) \times \\ & \prod_{i=j+1}^n (X_j^{q-1} - (X_i - \omega_i X_j)^{q-1}) \end{aligned}$$

be the indicatorfunction for ω (cf. [21]). The $\frac{q^{n+1}-1}{q-1}$ polynomial functions $f_\omega^d(X)$ are a basis for the space of homogeneous polynomials of degree d . Let $U = \{u_1, u_2, \dots, u_N\}$ be a set consisting of N distincts points of $\mathbb{P}^n(q)$. The function

$$f(X) = \sum_{\omega \notin U} f_\omega^d(X)$$

has exactly N zeros, namely the points of U . \square

Lemma 2.2. *For $n = 1$ and $d \leq q - 1$ the first and the second weight of the projective Reed-Muller code are respectively*

$$(3) \quad W_h^{(1)}(q, 1, d) = q - d + 1.$$

$$(4) \quad W_h^{(2)}(q, 1, d) = q - d + 2.$$

Proof. Let f a homogeneous polynomial in 2 variables of degree d where $2 \leq d \leq q - 1$. We can write

$$f(X_0, X_1) = X_0 g(X_0, X_1) + \lambda X_1^d.$$

where g is homogeneous of degree $d - 1$ and $\lambda \in \mathbb{F}_q$. Let us choose f such that $\lambda \neq 0$. If $X_0 = 0$ then $X_1 = 1$. Hence f has no zero for $X_0 = 0$. If $X_0 = 1$ then $f(1, X_1) = g(1, X_1) + \lambda X_1^d$. Hence $f(1, X_1)$ is a polynomial in one variable of degree d . Then it is possible to find f such that $f(1, X_1)$ has d zeros in \mathbb{F}_q . In this case $f(X_0, X_1)$ has d zeros in $\mathbb{P}^1(q)$.

Now let us choose f such that $\lambda = 0$. In this case $(0 : 1)$ is a solution and for $X_0 = 1$ we have $f(1, X_1) = g(1, X_1)$. Hence we can choose f such that $f(1, X_1) = g(1, X_1)$ has $d - 1$ zeros in \mathbb{F}_q . In this case $f(X_0, X_1)$ has also d zeros. We conclude that $W_h^{(1)}(q, 1, d) = (q + 1) - d$.

Remark that as $W_h^{(2)}(q, 1, d) > W_h^{(1)}(q, 1, d) = q - d + 1$ we have $W_h^{(2)}(q, 1, d) \geq q - d + 2$. It is straitforward, using for example

$$f(X_0, X_1) = X_0 g(X_0, X_1) + X_1^d$$

where $f(1, X_1)$ has $d - 1$ zeros in \mathbb{F}_q , to build a function $f(X_0, X_1)$ having $d - 1$ zeros. We conclude that $W_h^{(2)}(q, 1, d) = q - d + 2$. \square

In order to describe the minimal distance for the projective case, write $d - 1 = a(q - 1) + b$ with $0 \leq b < q - 1$. The minimum distance of a PGRM code was given by J.-P. Serre for $d \leq q$ (cf. [19]), and by A. Sørensen in [21] for the general case. The polynomials reaching the maximal number of zeros (or defining the minimum weighted codewords) are given by J.-P. Serre for $d \leq q$ (cf. [19]) and by the last author (cf. [16]) for the general case. Let us recall the following result stated in [16].

Theorem 2.3. *Let f be a homogeneous polynomial in $n + 1$ variables of total degree d , with coefficients in \mathbb{F}_q , which does not vanish on the whole projective space $\mathbb{P}^n(q)$. Then the following holds:*

- (1) *The number of \mathbb{F}_q -rational points $N_h(f)$ of the projective algebraic set defined by f satisfies the following:*

$$(5) \quad N_h(f) \leq \frac{q^{n+1} - 1}{q - 1} - W_h^{(1)}(q, n, d)$$

where

$$W_h^{(1)}(q, n, d) = \begin{cases} 1 & \text{if } d > n(q - 1), \\ (q - b)q^{n-a-1} & \text{if } d \leq n(q - 1), \end{cases}$$

with

$$d - 1 = a(q - 1) + b \text{ and } 0 \leq b < q - 1.$$

- (2) *The bound in (5) is attained. When $d \leq n(q-1)$, the polynomials f attaining this bound are exactly the polynomials defining an hypersurface $V = Z_h(f)$ such that: V contains a hyperplane H (namely f vanishes on H) and V restricted to the affine space $\mathbb{A}^n(q) = \mathbb{P}^n(q) \setminus H$ is a maximal affine hypersurface of $\mathbb{A}^n(q)$.*

Proof. The point (1) is proved by Sørensen in [21]. However, in order to prove at the same time the point (2) and to repair a flaw which is in the proof given in [16], let us rewrite entirely the proof given by Sørensen of the point (1) and let us show that one can deduce the result 2 from this proof.

If $d > n(q-1)$, as f does not vanish on the whole projective space $\mathbb{P}^n(q)$, then $N_h(f) \leq \frac{q^{n+1}-1}{q-1} - 1$. Lemma 2.1 proves that this bound is attained.

If $d \leq n(q-1)$ and $V = Z_h(f)$ contains a hyperplane H , we can suppose that this hyperplane is given by $X_0 = 0$, so that $f = X_0 f_1$, where f_1 is an homogeneous polynomial of degree $d-1$. The complement of H is the affine space

$$\mathbb{A}^n(q) = \{X \in \mathbb{P}^n(q) \mid X_0 = 1\}.$$

Let \tilde{f}_1 be the polynomial in n variables obtained from f_1 by setting $X_0 = 1$. This polynomial is defined on $\mathbb{A}^n(q)$ and does not vanish on the whole affine space $\mathbb{A}^n(q)$. Hence, using the result of Kasami and al. ([10]), we obtain:

$$N_a(\tilde{f}_1) \leq q^n - (q-b)q^{n-a-1},$$

and consequently

$$N_h(f) = \#H + N_a(\tilde{f}_1) \leq \frac{q^n - 1}{q - 1} + q^n - (q-b)q^{n-a-1},$$

$$N_h(f) \leq \frac{q^{n+1} - 1}{q - 1} - (q-b)q^{n-a-1},$$

where the symbol $\#$ denotes the cardinal. The bound is attained if and only if the polynomial \tilde{f}_1 verifies the conditions of maximality given in [6].

If $d \leq n(q-1)$ and $V = Z_h(f)$ does not contain any hyperplane, we give a proof of (5) by induction on n . If $n = 1$ and $d > q-1$ we know by Lemma 2.1 that the result is true. If $d \leq q-1$ the homogeneous polynomial f in two variables of degree d can be written:

$$f(X_0, X_1) = aX_1^d + bX_0g(X_0, X_1)$$

where $a \neq 0$ and $b \neq 0$ because V does not contain any hyperplane and where g is a non null homogeneous polynomial function of degree $d-1$. The point at infinity $X_0 = 0, X_1 = 1$ of the projective line is not a zero, then the only zeros are points such that $X_0 = 1$ and X_1 is solution of a polynomial equation in one variable of degree d . Then $N_h(f) \leq d$ and the induction property is verified.

Next suppose that the property is true for $n-1$ and $Z_h(f)$ does not contain any hyperplane. Then for any hyperplane H we have

$$\#(Z_h(f) \cap H) \leq \frac{q^n - 1}{q - 1} - W_h^{(1)}(q, n-1, d),$$

$$\#(H \setminus Z_h(f) \cap H) \geq W_h^{(1)}(q, n-1, d).$$

Let us count the number \mathcal{N} of couple (M, H) where H is a hyperplane and M a point in $(\mathbb{P}^n(q) \setminus Z_h(f)) \cap H$. We know that the number of hyperplanes containing a given point is $\frac{q^n-1}{q-1}$. Then

$$\mathcal{N} = \frac{q^n-1}{q-1} \#(\mathbb{P}^n(q) \setminus Z_h(f)).$$

This number is also the following sum on the $\frac{q^{n+1}-1}{q-1}$ hyperplanes of the space $\mathbb{P}^n(q)$

$$\mathcal{N} = \sum_H \#(H \setminus Z_h(f) \cap H) \geq \frac{q^{n+1}-1}{q-1} W_h^{(1)}(q, n-1, d).$$

Then

$$W_h(f) \geq \frac{q^{n+1}-1}{q^n-1} W_h^{(1)}(q, n-1, d),$$

$$W_h(f) > q W_h^{(1)}(q, n-1, d).$$

As $d \leq n(q-1)$ we have two cases:

- (1) $d \leq (n-1)(q-1)$ and then $W_h^{(1)}(q, n-1, d) = (q-b)q^{n-a-2}$. Hence $q W_h^{(1)}(q, n-1, d) = (q-b)q^{n-a-1} = W_h^{(1)}(q, n, d)$. In this case we conclude

$$W_h(f) > W_h^{(1)}(q, n, d),$$

which proves that the the induction property is verified and also that the bound cannot be reached by a hypersurface which does not contain any hyperplane.

- (2) $(n-1)(q-1) < d \leq n(q-1)$ and then $W_h^{(1)}(q, n-1, d) = 1$, $a = n-1$ and $W_h^{(1)}(q, n, d) = q-b$. Then

$$W_h(f) > q W_h^{(1)}(q, n-1, d) = q \geq q-b,$$

$$W_h(f) > W_h^{(1)}(q, n, d),$$

which proves that the the induction property is verified and also that the bound cannot be reached by a hypersurface which does not contain any hyperplane.

The point (2) is a consequence of the above reasoning.

□

3. THE SECOND WEIGHT IN THE AFFINE CASE

Let us denote by $W_a^{(2)}(q, n, d)$ the second weight of the GRM code $RM_q(d, n)$, namely the weight which is just above the minimum distance. Several simple cases can be easily described. If $d = 1$, we know that the code has only three weights: 0, the minimum distance $W_a^{(1)}(q, n, 1) = q^n - q^{n-1}$ and the second weight $W_a^{(2)}(q, n, 1) = q^n$. For $d = 2$ and $q = 2$ the weight distribution is more or less a consequence of the investigation of quadratic forms done by L. Dickson in [7] and was also done by E. Berlekamp and N. Sloane in an unpublished paper. For $d = 2$ and any q (including $q = 2$) the weight distribution was given by R. McEliece in [13]. For $q = 2$, for any n and any d , the weight distribution is known in the range $[W_a^{(1)}(2, n, d), 2.5W_a^{(1)}(2, n, d)]$ by a result of Kasami, Tokura, Azumi [11]. In particular, the second weight is $W_a^{(2)}(2, n, d) = 3 \times 2^{n-d-1}$ if $1 < d < n-1$ and

$W_a^{(2)}(2, n, d) = 2^{n-d+1}$ if $d = n-1$ or $d = 1$. For $d \geq n(q-1)$ the code $\text{RM}_q(d, n)$ is trivial, namely it is the whole $\mathcal{F}(q, d, n)$, hence any integer $0 \leq t \leq q^n$ is a weight.

The general problem of the second weight was tackled by D. Erickson in his thesis [8, 1974] and was partly solved. Unfortunately this very good piece of work was not published and remained virtually unknown. Meanwhile several authors became interested in the problem. The second weight was first studied by J.-P. Cherdieu and R. Rolland in [5] who proved that when $q > 2$ is fixed, for $d < q$ sufficiently small the second weight is

$$W_a^{(2)}(q, n, d) = q^n - dq^{n-1} + (d-1)q^{n-2}.$$

Their result was improved by A. Sboui in [18], who proved the formula for $d \leq q/2$. The methods in [5] and [18] are of a geometric nature by means of which the codewords reaching this weight were determined. These codewords are hyperplane arrangements. Then O. Geil in [9], using Gröbner basis methods, proved the formula for $d < q$. Moreover as an application of his method, he gave a new proof of the Kasami-Lin-Peterson minimum distance formula and determined, when $d > (n-1)(q-1)$, the first $d+1 - (n-1)(q-1)$ weights. In particular for $n = 2$ the problem is completely solved, and this case is particularly important as we shall see later. Finally, the last author in [17], using a mix of Geil's method and geometrical considerations found the second weight for all cases except when $d = a(q-1) + 1$. However the Gröbner basis method does not determine all the codewords reaching the second weight.

Recently, A. Bruen ([4]) exhumed the work of Erickson and completed the proof, solving the problem of the second weight for Generalized Reed-Muller code. Describe a little more the result of Erickson. First, in order to present his result introduce the following notation used in [8]: s and t are integers such that

$$d = s(q-1) + t, \text{ with } 0 < t \leq q-1.$$

Theorem 3.1. *The second weight $W_a^{(2)}(q, n, d)$ is*

$$W_a^{(2)}(q, n, d) = W_a^{(1)}(q, n, d) + cq^{n-s-2}$$

where $W_a^{(1)}(q, n, d) = (q-t)q^{n-s-1}$ is the minimal distance and c is

$$c = \begin{cases} q & \text{if } s = n-1 \\ t-1 & \text{if } s < n-1 \text{ and } 1 < t \leq \frac{q+1}{2} \\ & \text{or } s < n-1 \text{ and } t = q-1 \neq 1 \\ q & \text{if } s = 0 \text{ and } t = 1 \\ q-1 & \text{if } q < 4, s < n-2 \text{ and } t = 1 \\ q-1 & \text{if } q = 3, s = n-2 \text{ and } t = 1 \\ q & \text{if } q = 2, s = n-2 \text{ and } t = 1 \\ q & \text{if } q \geq 4, 0 < s \leq n-2 \text{ and } t = 1 \\ c_t & \text{if } q \geq 4, s \leq n-2 \text{ and } \frac{q+1}{2} < t \end{cases}$$

The number c_t is such that $c_t + (q-t)q$ is the second weight for the code $\text{RM}_q(2, t)$.

It results from the previous theorem that if one can compute the second weight for a case where $c = c_t$, the problem is completely solved. Alternatively, Erickson conjectured that $c_t = t-1$ and reduced this conjecture to a conjecture on blocking sets [8, Conjecture 4.14 p. 76]. Recently in [4] A. Bruen proved that this conjecture follows from two of his papers [2], [3]. Then the problem is now solved by [8]+[4].

It is also solved by [8]+[9] (the important case $n = 2$ is completely solved in [9] and this leads to the conclusion as noted above) or by [8]+[17] (the cases not solved in [8] are explicitly resolved in [17]). More precisely

Theorem 3.2. *The coefficient c_t used in the previous theorem 3.1 is*

$$c_t = t - 1.$$

Remark 3.3. The values s and t are connected to the values a and b of the formula (1) in the following way: $a = s$ and $b = t$ unless $t = q - 1$ and in this case $a = s + 1$ and $b = 0$. Let us also express the second weight with the classical writing (1) for the Euclidean quotient (cf. [17]):

The second weight is given by the following:

I) $n = 1$ (and then $q > 2$):

$$W_a^{(2)}(q, n, d) = q - d + 1;$$

II) $n \geq 2$

A) $d = 1$:

$$W_a^{(2)}(q, n, d) = q^n;$$

B) $d \geq 2$

1) $q = 2$

a) $2 \leq d < n - 1$:

$$W_a^{(2)}(q, n, d) = 3 \times 2^{n-d-1};$$

b) $d = n - 1$:

$$W_a^{(2)}(q, n, d) = 4;$$

2) $q \geq 3$

a) $2 \leq d < q$:

$$W_a^{(2)}(q, n, d) = q^n - dq^{n-1} + (d-1)q^{n-2};$$

b) $(n-1)(q-1) < d < n(q-1)$:

$$W_a^{(2)}(q, n, d) = q - b + 1;$$

c) $q \leq d \leq (n-1)(q-1)$

i) $b = 0$:

$$W_a^{(2)}(q, n, d) = 2q^{n-a-1}(q-1);$$

ii) $b = 1$

α) $q = 3$

$$W_a^{(2)}(3, n, d) = 8 \times 3^{n-a-2};$$

β) $q \geq 4$:

$$W_a^{(2)}(q, n, d) = q^{n-a};$$

iii) $2 \leq b < q - 1$:

$$W_a^{(2)}(q, n, d) = q^{n-a-2}(q-1)(q-b+1).$$

Finally let us remark that we now have several approaches, close to each other, but nevertheless different. The first one [8],[4] is mainly based on combinatorics of finite geometries, the second one [5],[18], [17] is mainly based on geometry and hyperplane arrangements, the third [9], [17] is mainly based on polynomial study by means of commutative algebra and Gröbner basis. All these approaches can be fruitful for the study of similar problems.

The polynomials reaching the second weight are known for $2d \leq q$ (cf. [8, Theorem 3.13, p. 60], [18]). For the other values of d the result is not known. However we can say that:

Theorem 3.4. *If $f \in \mathcal{RP}(q, n, d)$ is an irreducible polynomial but not absolutely irreducible, in n variables over \mathbb{F}_q , of degree $d > 1$ then the weight $W_a(f)$ of the corresponding codeword in $\text{RM}_q(n, d)$ is such that $W_a(f) > W_a^{(2)}(q, n, d)$.*

Proof. The tedious proof is postponed in Appendix A. \square

Theorem 3.5. *If $f \in \mathcal{RP}(q, n, d)$ is a product of two polynomials $f = g \cdot h$ such that*

- (1) $2 \leq d' = \deg(g) \leq d = \deg(f) < q - 1$;
- (2) g is irreducible but not absolutely irreducible;

then $W_a(f) > W_a^{(2)}(q, n, d)$.

Proof. The number of zeros of f is such that $N_a(f) \leq N_a(g) + N_a(h)$. By Lemma A.2 (cf. Appendix) the following holds:

$$N_a(g) < \frac{d'}{2}q^{n-1}.$$

The number of zeros of h can be bounded by the maximum number of zeros for a non-null polynomial function:

$$N(h) \leq (d - d')q^{n-1}.$$

Then

$$N_a(f) < (d - d' + \frac{d'}{2})q^{n-1}.$$

But $\frac{d'}{2} \geq 1$, then

$$N_a(f) < (d - 1)q^{n-1} = dq^{n-1} - q^{n-1},$$

and as $d - 1 < q$ the following holds:

$$N_a(f) < dq^{n-1} - (d - 1)q^{n-2} = q^n - W_a^{(2)}(q, n, d).$$

\square

Remark 3.6. In any case, among the words reaching the second distance, there are hyperplane configurations. For example the hyperplane configurations given in [17].

4. THE SECOND WEIGHT IN THE PROJECTIVE CASE

In this section we tackle the unsolved problem of finding the second weight $W_h^{(2)}(q, n, d)$ for GPRM codes.

Lemma 4.1. *Let f be a homogeneous polynomial in $n+1$ variables of total degree d , with coefficients in \mathbb{F}_q , which does not vanish on the whole projective space $\mathbb{P}^n(q)$. If there exists a projective hyperplane H such that the affine hypersurface $(\mathbb{P}^n(q) \setminus H) \cap Z_h(f)$ contains an affine hyperplane of the affine space $\mathbb{A}^n(q) = \mathbb{P}^n(q) \setminus H$ then the projective hypersurface $Z_h(f)$ contains a projective hyperplane. In particular if f restricted to the affine space $\mathbb{A}^n(q)$ defines a maximal affine hypersurface then $Z_h(f)$ contains a hyperplane.*

Proof. Suppose that

$$f(1, X_1, \dots, X_n) = (l(X_1, \dots, X_n) - \alpha) f_1(X_1, \dots, X_n)$$

where $l(X_1, \dots, X_n)$ is linear, then

$$\begin{aligned} f(X_0, X_1, \dots, X_n) &= \\ (l(X_1, \dots, X_n) - \alpha X_0) \tilde{f}_1(X_0, X_1, \dots, X_n) \end{aligned}$$

where $\tilde{f}_1(X_0, X_1, \dots, X_n)$ is the homogeneous polynomial obtained by homogenization of $f_1(X_1, \dots, X_n)$. We conclude that f defines a hypersurface containing a hyperplane. \square

Lemma 4.2. *For $n \geq 2$ the following holds*

$$W_h^{(1)}(q, n-1, d) + W_a^{(2)}(q, n, d) \leq W_a^{(2)}(q, n, d-1).$$

Proof. Let us introduce the following notations:

$$d-1 = s_{d-1}(q-1) + t_{d-1},$$

where $1 \leq t_{d-1} \leq q-1$;

$$d = s_d(q-1) + t_d,$$

where $1 \leq t_d \leq q-1$.

$$c(d-1) \text{ and } c(d)$$

are the values of the coefficient c which occurs in Theorem 3.1, with respect to $d-1$ and d . Then we have

$$\begin{aligned} W_h^{(1)}(q, n-1, d) &= (q - t_{d-1})q^{n-s_{d-1}-2}, \\ W_a^{(2)}(q, n, d) &= (q - t_d)q^{n-s_d-1} + c(d)q^{n-s_d-2}, \\ W_a^{(2)}(q, n, d-1) &= (q - t_{d-1})q^{n-s_{d-1}-1} + c(d-1)q^{n-s_{d-1}-2}. \end{aligned}$$

Denote by Δ the difference

$$\begin{aligned} \Delta &= W_a^{(2)}(q, n, d-1) \\ &\quad - \left(W_h^{(1)}(q, n-1, d) + W_a^{(2)}(q, n, d) \right) \end{aligned}$$

- If $1 \leq t_{d-1} \leq q-2$ then $q > 2$, $t_d = t_{d-1} + 1$ and $s_d = s_{d-1}$. In this case let us denote by s the common value of s_d and s_{d-1} . Hence

$$\Delta = q^{n-s-2} (t_{d-1} + c(d-1) - c(d)).$$

- If $s = n-1$ then $c(d-1) = c(d) = q$ and $\Delta > 0$.
- If $s < n-1$ and $1 < t_{d-1} \leq \frac{q+1}{2} - 1$ then $q \geq 4$ and $c(d-1) - c(d) = -1$. Hence $\Delta > 0$.
- If $s < n-1$ and $\frac{q+1}{2} - 1 < t_{d-1} \leq \frac{q+1}{2}$ then $q \geq 4$ and $c(d-1) - c(d) = -1$. Hence $\Delta > 0$.
- If $s < n-1$, $q \geq 4$ and $t_{d-1} = 1$ then $c(d-1) - c(d) = q - t_{d-1}$. Hence $\Delta > 0$.
- If $s < n-1$, $q = 3$ and $t_{d-1} = 1$ then $c(d-1) - c(d) = 1$. Hence $\Delta > 0$.
- If $t_{d-1} = q-1$ then $t_d = 1$ and $s_d = s_{d-1} + 1$. Hence

$$\Delta = q^{n-s_{d-1}-3} (c(d-1)q - c(d)) \geq 0.$$

\square

Remark 4.3. In the previous lemma, equality holds if and only if $t_{d-1} = q - 1$, $c(d-1) = 1$ and $c(d) = q$.

For $q > 3$ this case cannot happen.

For $q = 2$, $c(d-1)$ can be 1 if and only if $s_{d-1} < n - 2$. In this case, c_d is q if and only if $s_d = n - 2$. Then for $q = 2$ the equality holds if and only if $s_{d-1} = n - 3$ (note that for $q = 2$ we always have $t_{d-1} = 1$). Namely:

$$d - 1 = (n - 3)(q - 1) + 1.$$

For $q = 3$, $c(d-1)$ can be 1 if and only if $t_{d-1} = 2$ and $s_{d-1} < n - 1$. Moreover in this case $c(d) = q$ if and only if $s_d = n - 1$. Then for $q = 3$ the equality holds if and only if $t_{d-1} = 2$ and $s_{d-1} = n - 2$. Namely:

$$d - 1 = (n - 2)(q - 1) + 2.$$

Theorem 4.4. Let $W_h^{(2)}(q, n, d)$ be the second weight for a homogeneous polynomial f in $n + 1$ variables ($n \geq 2$) of total degree d , with coefficients in \mathbb{F}_q , which is not maximal. Let us define $V_h^{(2)}(q, n, d)$ by:

$$V_h^{(2)}(q, n, d) = 2$$

if $d > n(q - 1)$ and

$$(6) \quad V_h^{(2)}(q, n, d) = W_h^{(1)}(q, n - 1, d) + W_a^{(2)}(q, n, d),$$

if $d \leq n(q - 1)$. Then the following holds

$$V_h^{(2)}(q, n, d) \leq W_h^{(2)}(q, n, d) \leq W_a^{(2)}(q, n, d - 1).$$

Proof. Let us remark first that by Lemma 4.2

$$V_h^{(2)}(q, n, d) \leq W_a^{(2)}(q, n, d - 1).$$

If $d > n(q - 1)$, as f does not vanish on the whole projective space $\mathbb{P}^n(q)$, and f is not maximal then $N_h(f) \leq \frac{q^{n+1}-1}{q-1} - 2$. Lemma 2.1 proves that this bound is attained. Then in this case $W_h^{(2)}(q, n, d) = 2$.

Suppose now that $2 \leq d \leq n(q - 1)$. Let f such that $Z_h(f)$ is not maximal. Suppose first that there is an hyperplane H in $Z_h(f)$. Then we can suppose that

$$f(X_0, X_1, \dots, X_n) = X_0 g(X_0, X_1, \dots, X_n)$$

where g is an homogeneous polynomial of degree $d - 1$. The function

$$f_1(X_1, \dots, X_n) = g(1, X_1, \dots, X_n)$$

defined on the affine space $\mathbb{A}^n(q) = \mathbb{P}^n(q) \setminus H$ is a polynomial function in n variables of total degree $d - 1$. If it was maximum, by Theorem 2.3, the function f would also be maximum.

Then $\#Z_a(f_1) \leq q^n - W_a^{(2)}(q, n, d - 1)$. Hence the following holds:

$$\begin{aligned} \#Z_h(f) &\leq \frac{q^n - 1}{q - 1} + q^n - W_a^{(2)}(q, n, d - 1), \\ \#Z_h(f) &\leq \frac{q^{n+1} - 1}{q - 1} - W_a^{(2)}(q, n, d - 1), \end{aligned}$$

and the equality holds if and only if f_1 reaches the second weight on the affine space $\mathbb{A}^n(q)$. This case actually occurs. Hence for such a word, in general we have

$$W_h(f) \geq W_a^{(2)}(q, n, d - 1),$$

and as the equality occurs, the following holds for the second distance: $W_h^{(2)}(q, n, d) \leq W_a^{(2)}(q, n, d-1)$.

Suppose now that there is not any hyperplane in the hypersurface $Z_h(f)$. Let H be a hyperplane and $\mathbb{A}^n(q) = \mathbb{P}^n(q) \setminus H$. Then as $H \cap Z_h(f) \neq H$

$$\#(H \cap Z_h(f)) \leq \frac{q^n - 1}{q - 1} - W_h^{(1)}(q, n - 1, d),$$

and by Lemma 4.1

$$\#(Z_h(f) \cap \mathbb{A}^n(q)) \leq q^n - W_a^{(2)}(q, n, d).$$

Then

$$\begin{aligned} \#Z_h(f) &\leq \frac{q^n - 1}{q - 1} - W_h^{(1)}(q, n - 1, d) \\ &\quad + q^n - W_a^{(2)}(q, n, d) \\ &\leq \frac{q^{n+1} - 1}{q - 1} \\ &\quad - \left(W_h^{(1)}(q, n - 1, d) + W_a^{(2)}(q, n, d) \right) \end{aligned}$$

and consequently

$$W_h(f) \geq W_h^{(1)}(q, n - 1, d) + W_a^{(2)}(q, n, d).$$

Then, for the second distance the conclusion of the theorem holds. \square

Open question. What is the exact value of $W_h^{(2)}(q, n, d)$? This question remains open. However let us remark that if $2d \leq q$ we know all the words reaching the affine second distance. Each hypersurface associated to one of these words is a hyperplane configuration. Then, by Lemma 4.1 we conclude that

$$W_h^{(2)}(q, n, d) \geq W_h^{(1)}(q, n - 1, d) + W_a^{(3)}(q, n, d).$$

Unfortunately we don't know $W_a^{(3)}(q, n, d)$ and we don't know if $W_h^{(1)}(q, n - 1, d) + W_a^{(3)}(q, n, d)$ is greater than $W_a^{(2)}(q, n, d - 1)$ or not.

APPENDIX A. PROOF OF THEOREM 3.4

The proof of Theorem 3.4 is based on the two following lemmas. The first one is a key lemma which can be found in [20]. The second one is a slight modification of [16, Theorem 2.1].

Lemma A.1. *Let f be a non-zero irreducible but not absolutely irreducible polynomial over the finite field \mathbb{F}_q , in n variables and of degree d . Then one can find a finite extension $\mathbb{F}_{q'}$ such that there exists a unique polynomial g absolutely irreducible over the finite field $\mathbb{F}_{q'}$, in n variables and of degree d' , satisfying:*

$$f = \prod_{\sigma \in G} g^\sigma,$$

where $G = \text{Gal}(\mathbb{F}_{q'}/\mathbb{F}_q)$ is the Galois group of $\mathbb{F}_{q'}$ over \mathbb{F}_q and

$$\text{Deg}(f) = [\mathbb{F}_{q'} : \mathbb{F}_q] \text{Deg}(g).$$

Lemma A.2. *Let $f \in \mathcal{RP}(q, n, d)$ be an irreducible but not absolutely irreducible polynomial of degree $d > 1$. Let us set a and b such that $d = a(q-1) + b$ and $0 \leq b < q-1$. Denote by u a number less than or equal to the smallest prime factor of d . Then the number $N_a(f)$ of zeros of f over \mathbb{F}_q satisfies:*

$$(7) \quad N_a(f) < q^n - 2q^{n - \lfloor \frac{d}{u(q-1)} \rfloor - 1}.$$

Moreover if $a = 0$

$$(8) \quad N_a(f) < \frac{d}{u} q^{n-1}.$$

Proof. Using the lemma A.1 we get:

$$Z_a(f) = \bigcup_{\sigma \in G} Z_a(g^\sigma).$$

However all the conjugate polynomials g^σ have the same zeros in \mathbb{F}_q . Hence $Z_a(f) = Z_a(g)$.

Let us denote by s the dimension $[\mathbb{F}_{q'} : \mathbb{F}_q]$ of the vector space $\mathbb{F}_{q'}$ over the field \mathbb{F}_q . We know that:

$$d = \text{Deg}(f) = s \text{Deg}(g) = sd'.$$

If (w_1, \dots, w_s) is a basis of $\mathbb{F}_{q'}$ over \mathbb{F}_q :

$$g(X) = \sum_{j=1}^s h_j(X) w_j,$$

where $h_j \in \mathcal{RP}(q, d', n)$ and are not all zero. Hence,

$$Z_a(f) = \bigcap_{j=1}^s Z_a(h_j).$$

All the non-zero h_j cannot be the same products of degree one polynomials (in this case, g would be proportional to a polynomial over \mathbb{F}_q), so that, by the result of Delsarthe, Goethals, McWilliams [6], $\#Z_a(f)$ cannot attain the maximum number of zeros given by the formula of Kasami, Lin, Peterson ([10]):

$$\#Z_a(f) < q^n - (q - b')q^{n-a'-1}$$

where $d' = a'(q-1) + b'$ and $0 \leq b' < q-1$. But a' is the integer part of $d'/q-1$, namely:

$$a' = \left\lfloor \frac{d'}{q-1} \right\rfloor = \left\lfloor \frac{d}{s(q-1)} \right\rfloor.$$

In any case:

$$\#Z_a(f) < q^n - (q - (q-2))q^{n - \lfloor \frac{d}{s(q-1)} \rfloor - 1}.$$

As s divides d we have $u \leq s$ and consequently

$$\#Z_a(f) < q^n - 2q^{n - \lfloor \frac{d}{u(q-1)} \rfloor - 1}.$$

Now, if $a = 0$ then $a' = 0$ and we can improve the previous estimate. In this case we know that $b' = d' = d/s$, so that:

$$\#Z_a(f) < q^n - (q - d/s)q^{n-1}.$$

As s divides d we have $u \leq s$ and consequently the following inequality holds:

$$\#Z_a(f) < \frac{d}{s} q^{n-1} \leq \frac{d}{u} q^{n-1}.$$

Let us remark that $2 \leq u$ so that if we replace u by 2, formulas are still valid. \square

Proof of Theorem 3.4

By Lemma A.2 the weight $W_a(f)$ of the codeword associated to f is such that

$$(9) \quad W_a(f) > 2q^{n - \lfloor \frac{d}{u(q-1)} \rfloor - 1}.$$

Moreover when $a = 0$ the following holds:

$$(10) \quad W_a(f) > q^n - \frac{d}{u}q^{n-1}.$$

In general we shall apply this result with $u = 2$ unless we have more information on d and if we need a more accurate inequality. In the following we compare for any case $W_a(f)$ to $W_a^{(2)}(q, n, d)$ and we prove that $W_a(f) > W_a^{(2)}(q, n, d)$.

For $n = 1$ the result is trivial (f does not have any zero). We suppose now that $n \geq 2$. Subsequently a_2 is defined by:

$$a_2 = \left\lfloor \frac{d}{u(q-1)} \right\rfloor,$$

with $u = 2$ unless we specify another value.

A.1. The case $q = 2$.

- $2 \leq d < n - 1$. We know that $W_a^{(2)}(q, n, d) = 3 \times 2^{n-d-1}$. As $d \geq 2$, we have $a_2 = \left\lfloor \frac{d}{2(q-1)} \right\rfloor \geq 1$. If d is even then $2a_2 = d$ and the following holds:

$$\begin{aligned} W_a^{(2)}(q, n, d) &= 3 \times 2^{n-2a_2-1} \leq 3 \times 2^{n-a_2-2} \\ &\leq \frac{3}{4} \times 2^{n-a_2} < \frac{3}{4} W_a(f). \end{aligned}$$

If d is odd, then $a_2 = \frac{d-1}{2}$ and $d = 2a_2 + 1$. It follows that $W_a(f) > 4 \times 2^{n-a_2-2} > 3 \times 2^{n-2a_2-2} = W_a^{(2)}(q, n, d)$.

- $d = n - 1$. Then $W_a^{(2)}(q, n, d) = 4$. As $d \geq 2$ we conclude that $n \geq 3$ and $a_2 = \left\lfloor \frac{n-1}{2} \right\rfloor \leq \frac{n-1}{2}$. Then

$$W_a(f) > 2^{n-a_2} \geq 2^{\frac{n+1}{2}} \geq 4 = W_a^{(2)}(q, n, d).$$

A.2. The case $q \geq 3$ and $2 \leq d < q$.

- $2 \leq d < q - 1$. Here $a = 0$. Then $W_a(f) > q^n - \frac{d}{2}q^{n-1}$. On the other hand, $W_a^{(2)}(q, n, d) = q^n - dq^{n-1} + (d-1)q^{n-2}$. Then

$$W_a(f) - W_a^{(2)}(q, n, d) > \frac{d}{2}q^{n-1} - (d-1)q^{n-2},$$

$$W_a(f) - W_a^{(2)}(q, n, d) > q^{n-2} \left(\frac{qd}{2} - d + 1 \right).$$

But $q \geq 3$ then $\frac{qd}{2} \geq \frac{3}{2}d$ and

$$W_a(f) - W_a^{(2)}(q, n, d) > 2q^{n-2}.$$

- $d = q - 1$. In this case $W_a^{(2)}(q, n, d) = 2q^{n-1} - 2q^{n-2}$ while $a_2 = \left\lfloor \frac{1}{2} \right\rfloor = 0$ and $W_a(f) > 2q^{n-1}$. Hence

$$W_a(f) - W_a^{(2)}(q, n, d) > 2q^{n-2}.$$

A.3. The case $q \geq 3$ and $(n-1)(q-1) < d < n(q-1)$. In this case $a_2 < \frac{n}{2}$, $W_a^{(2)}(q, n, d) = (q-b+1)$. On the other hand, $W_a(f) > 2q^{n-a_2-1}$. If $n = 2$ then $a_2 = 0$ and $W_a(f) > 2q > W_a^{(2)}(q, n, d)$. If $n = 3$ then $a_2 = 1$ and $W_a(f) > 2q^{n-2} \geq 2q > W_a^{(2)}(q, n, d)$. If $n \geq 4$ then $W_a(f) > q^{\frac{n-2}{2}} \geq 2q > W_a^{(2)}(q, n, d)$.

A.4. The case $q \geq 3$ and $q \leq d \leq (n-1)(q-1)$.

A.4.1. $b = 0$. In this case $W_a^{(2)}(q, n, d) = 2q^{n-a-1}(q-1)$ and $a_2 = \lfloor \frac{a}{2} \rfloor$. If a is even then $a = 2a_2 \geq 1$. Then $W_a^{(2)}(q, n, d) = 2q^{n-2a_2} - 2q^{n-2a_2-1}$ and $W_a(f) > 2q^{n-a_2-1}$. Hence,

$$W_a(f) - W_a^{(2)}(q, n, d) > 2q^{n-2a_2} (q^{a_2-1} - 1) + 2q^{n-2a_2-1}.$$

As $q^{a_2-1} - 1 \geq 0$ we conclude that

$$W_a(f) - W_a^{(2)}(q, n, d) > 2q^{n-a-1}.$$

If a is odd then $a = 2a_2 + 1$ and $W_a^{(2)}(q, n, d) = 2q^{n-2a_2-1} - 2q^{n-2a_2-2}$. The following formulas hold:

$$w(f) - W_a^{(2)}(q, n, d) > 2q^{n-2a_2-1} (q^{a_2} - 1) + 2q^{n-2a_2-2}.$$

As $q^{a_2} - 1 \geq 0$ we conclude that

$$w(f) - W_a^{(2)}(q, n, d) > 2q^{n-a-1}.$$

A.4.2. $b = 1$.

- $q = 3$. In this case $d = 2a + 1$, and consequently the lowest prime factor of d is ≥ 3 . Then we shall take $u = 3$ for this case. Hence $a_2 = \lfloor \frac{d}{3(q-1)} \rfloor = \lfloor \frac{d}{6} \rfloor < \frac{d}{6}$, namely $a_2 < \frac{a}{3} + \frac{1}{6}$. Moreover $W_a^{(2)}(q, n, d) = 8 \times 3^{n-a-2}$ and $W_a(f) > 2 \times 3^{n-\frac{a}{3}-\frac{1}{6}-1}$. Then

$$W_a(f) - W_a^{(2)}(q, n, d) > 2 \times 3^{n-a-2} \left(3^{\frac{2a}{3} + \frac{5}{6}} - 4 \right)$$

and as $a \geq 1$

$$\begin{aligned} W_a(f) - W_a^{(2)}(q, n, d) &> 2 \times 3^{n-a-2} \left(3^{\frac{3}{2}} - 4 \right) \\ &> 2 \times 3^{n-a-2}. \end{aligned}$$

- $q \geq 4$. We know that $W_a^{(2)}(q, n, d) = q^{n-a}$ and $W_a(f) > 2q^{n-a-1}$. If $a_2 = 0$ then

$$W_a(f) - W_a^{(2)}(q, n, d) > 2q^{n-1} - q^{n-a} \geq q^{n-1}.$$

If $a = 1$ then $d = q \geq 4$ and $a_2 \leq \frac{q}{2(q-1)} \leq \frac{2}{3} < 1$. Then $a_2 = 0$. Hence, if $a_2 = 1$ then $a \geq 2$. Then $W_a(f) > q^{n-2}$ and $W_a^{(2)}(q, n, d) \leq q^{n-2}$. We conclude that

$$W_a(f) - W_a^{(2)}(q, n, d) > 0.$$

If $a_2 \geq 2$, we know that $a_2 = \lfloor \frac{a(q-1)+1}{2(q-1)} \rfloor$ and then $a_2 \leq \frac{a}{2} + \frac{1}{6}$ or $a > 2a_2 - \frac{1}{3}$.

Consequently $W_a^{(2)}(q, n, d) < q^{n-2a_2+\frac{1}{3}}$ while $W_a(f) > 2q^{n-a_2-1}$, hence

$$W_a(f) - W_a^{(2)}(q, n, d) > q^{n-2a_2+\frac{1}{3}} \left(2q^{a_2-\frac{4}{3}} - 1 \right) > 0.$$

A.4.3. $2 \leq b < q - 1$. We know that $W_a^{(2)}(q, n, d) = q^{n-a-2}(q-1)(q-b+1)$. From the definitions we get the two following inequalities:

$$\frac{d}{q-1} - 1 < a \leq \frac{d}{q-1},$$

$$\frac{d}{2(q-1)} - 1 < a_2 \leq \frac{d}{2(q-1)},$$

then

$$0 \leq a - 2a_2 \leq 1.$$

If a is even then $a = 2a_2 \geq 2$ and

$$W_a^{(2)}(q, n, d) = q^{n-2a_2-2}(q-1)(q-b+1) < q^{n-2a_2}.$$

Hence:

$$W_a(f) - W_a^{(2)}(q, n, d) > 2q^{n-a_2-1} - q^{n-2a_2},$$

$$W_a(f) - W_a^{(2)}(q, n, d) > q^{n-2a_2} (2q^{a_2-1} - 1),$$

and as $a_2 \geq 1$ we conclude that

$$W_a(f) - W_a^{(2)}(q, n, d) > q^{n-2a_2}.$$

If a is odd, $a = 2a_2 + 1$, $a \geq 1$, $a_2 \geq 0$. Moreover

$$W_a^{(2)}(q, n, d) = q^{n-2a_2-3}(q-1)(q-b+1) < q^{n-2a_2-1}$$

and

$$W_a(f) > 2q^{n-a_2-1}.$$

Then

$$W_a(f) - W_a^{(2)}(q, n, d) > q^{n-2a_2-1} (2q^{a_2} - 1),$$

and as $2q^{a_2} - 1 \geq 1$ we obtain

$$W_a(f) - W_a^{(2)}(q, n, d) > q^{n-2a_2-1}.$$

REFERENCES

- [1] I. Blake and R. Mullin, *The mathematical theory of coding*. Academic Press, 1975.
- [2] A. Bruen, "Polynomial multiplicities over finite fields and intersection sets," *Journal of combinatorial theory*, vol. 60, no. 1, pp. 19–33, 1992.
- [3] —, "Applications of finite fields to combinatorics and finite geometries," *Acta Applicandae Mathematicae*, vol. 93, no. 1–3, 2006.
- [4] —, "Blocking sets and low-weight codewords in the generalized reed-muller codes," in *Error-correcting Codes, Finite Geometries, and Cryptography*, ser. Contemporary Mathematics, A. Bruen, D. Wehlau, and C. M. Society, Eds., vol. 525. American Mathematical Society, 2010, pp. 161–164.
- [5] J.-P. Cherdieu and R. Rolland, "On the number of points of some hypersurfaces in \mathbb{F}_q^n ," *Finite Field and their Applications*, vol. 2, pp. 214–224, 1996.
- [6] P. Delsarte, J. Goethals, and F. MacWilliams, "On generalized reed-muller codes and their relatives," *Information and Control*, vol. 16, pp. 403–442, 1970.
- [7] L. Dickson, *Linear groups*. Dover Publications, 1958.
- [8] D. Erickson, "Counting zeros of polynomials over finite fields," Ph.D. dissertation, Thesis of the California Institute of Technology, Pasadena California, 1974.
- [9] O. Geil, "On the second weight of generalized Reed-Muller codes," *Designs, Codes and Cryptography*, vol. 48, no. 3, pp. 323–330, 2008.
- [10] T. Kasami, S. Lin, and W. Peterson, "New generalizations of the reed-muller codes part i: primitive codes," *IEEE Transactions on Information Theory*, vol. IT-14, no. 2, pp. 189–199, March 1968.
- [11] T. Kasami, N. Tokura, and S. Azumi, "On the weight enumeration of weights less than 2.5d of Reed-Muller codes," *Information and Control*, vol. 30, no. 4, pp. 380–395, April 1976.

- [12] G. Lachaud, “Projective reed-muller codes,” in *Coding Theory and Applications*, ser. Lecture Notes in Computer Science, no. 311. Springer-Verlag, 1988, pp. 125–129.
- [13] R. McEliece, “Quadratic forms over finite fields and second-order Reed-Muller codes,” JPL Space Programs Summary III, Tech. Rep., 1969.
- [14] D.-J. Mercier and R. Rolland, “Polynômes homogènes qui s’annulent sur l’espace projectif $\mathbb{P}^m(\mathbb{F}_q)$,” *Journal of pure and applied algebra*, vol. 124, pp. 227–240, 1998.
- [15] C. Rentería and H. Tapia-Recillas, “Reed-muller codes: An ideal theory approach,” *Communications in algebra*, vol. 25, no. 2, pp. 401–413, 1997.
- [16] R. Rolland, “Number of points of non-absolutely irreducible hypersurfaces,” in *Algebraic geometry and its applications*, ser. Number Theory and Its Applications, J. Hirschfeld, J. Chaumine, and R. Rolland, Eds., vol. 5. World Scientific, 2008, pp. 481–487, proceedings of the first SAGA conference, 7-11 May 2007, Papeete.
- [17] —, “The second weight of generalized reed-muller codes in most cases,” *Cryptography and Communications – Discrete Structures, Boolean Functions and Sequences*, vol. 2, no. 1, pp. 19–40, 2010.
- [18] A. Sboui, “Second highest number of points of hypersurfaces in \mathbb{F}_q^n ,” *Finite Fields and Their Applications*, vol. 13, no. 3, pp. 444–449, July 2007.
- [19] J.-P. Serre, “Lettre à m. tsfasman du 24 juillet 1989,” in *Journées arithmétiques de Luminy 17–21 Juillet 1989*, ser. Astérisque. Société Mathématique de France, 1991, pp. 198–200.
- [20] A. Sorensen, “A note on algorithms deciding rationality and absolutely irreducibility based on the number of rational solutions,” *RISC-Linz, Series*, 91-37.0, August 1991.
- [21] A. Sorensen, “projective reed-muller codes,” *Transactions on Information Theory*, vol. IT-37, no. 6, pp. 1567–1576, 1991.

INSTITUT DE MATHÉMATIQUES DE LUMINY, CASE 930, F13288 MARSEILLE CEDEX 9, FRANCE
E-mail address: `stephane.ballet@univmed.fr`

INSTITUT DE MATHÉMATIQUES DE LUMINY, CASE 930, F13288 MARSEILLE CEDEX 9, FRANCE
E-mail address: `robert.rolland@acrypta.fr`